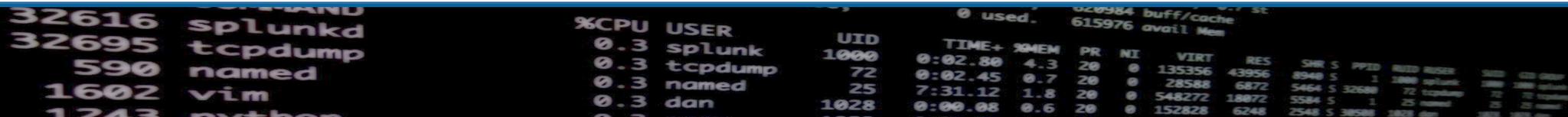


# What's New in Splunk 9.0

Dave Shpritz, Aplura Director of Services

Baltimore Splunk User Group

July 2022



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, USER, TTY, TIME, CMD. The process list includes splunkd, tcpdump, named, vim, and python.

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	USER	TTY	TIME	CMD
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	/usr/local/splunk/bin	splunk		0:00.00	splunkd
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	/usr/local/sbin	tcpdump		0:00.00	tcpdump
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/usr/sbin	named		0:00.00	named
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	/usr/bin	python		0:00.00	python



# Agenda

- Overview
- Security
- Indexing
- Admin
- Search
- Other stuff

```
02:09:84 buff/cache 0 used, 615976 avail Mem
```

PID	PPID	USER	%CPU	MEM	TIME	PR	NI	VIRT	RES	SHR	S	PPID	USER	%CPU	MEM	TIME	PR	NI	VIRT	RES	SHR	S	
32616		splunkd	0.3		0:02.80	20	0	135356	43956	8940	S	1	splunkd	0.3		0:02.45	20	0	28588	6872	5464	S	1
32695		tcpdump	0.3		7:31.12	20	0	548272	18872	5584	S	1	tcpdump	0.3		0:00.08	20	0	152828	6248	2548	S	1
590		named	0.3										named	0.3									
1602		vim	0.3										vim	0.3									
1243		python	0.3										python	0.3									

# Overview - Splunk Version 9.0.0

- Released at .conf22
- Release Notes:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/MeetSplunk>
- Upgrade:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/Installation/AboutupgradingREADTHISFIRST>
- Known Issues:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/Knownissues>

```
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSSD  RSSM  RSSV  RSSO  RSSP  RSSC  RSSD  RSSM  RSSV  RSSO  RSSP  RSSC
0.3  splunk  1000    0:02.80  4.3  20  0  135356  43956  8940  S   1  2880  2880  2880  2880  2880  2880  2880  2880  2880  2880  2880  2880  2880
0.3  tcpdump  72     0:02.45  0.7  20  0  28588  6872  5464  S  32689  72  72  72  72  72  72  72  72  72  72  72  72  72
0.3  named    25     7:31.12  1.8  20  0  548272  18872  5584  S   1  25  25  25  25  25  25  25  25  25  25  25  25  25
0.3  dan     1028    0:00.08  0.6  20  0  152828  6248  2548  S  38588  1828  1828  1828  1828  1828  1828  1828  1828  1828  1828  1828  1828  1828
```

# Security

```
020984 buff/cache 0 used, 615976 avail Mem
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR S  PPID  RSS  RSIZE  STATE  COMMAND
0.3 splunk    1000    0:02.80 4.3  20  0  135356 43956 8940 S  1  2880  1000  1000  splunk
0.3 tcpdump   72     0:02.45 0.7  20  0  28588  6872  5464 S  72  1000  1000  1000  tcpdump
0.3 named     25     7:31.12 1.8  20  0  548272 18872 5584 S  1  25  1000  1000  named
0.3 dan      1028    0:00.08 0.6  20  0  152828  6248  2548 S  38584 1828  1000  1000  dan
```



# Security

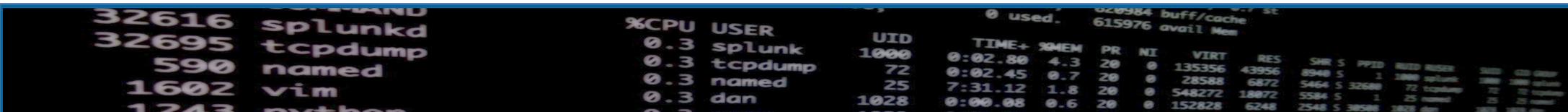
- Security vulnerabilities
- TLS changes
- Audit improvements/Config Tracking
- Universal Forwarder
- Role-based fields

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	PID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	PPID	PID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S		
32616	32616	splunkd	0.3	0.3	0:02.80	20	0	135356	43956	8940	S	1	32695	32695	tcpdump	0.3	0.3	0:02.45	20	0	28588	6872	5464	S	1
590	590	named	0.3	0.3	7:31.12	20	0	548272	18872	5584	S	1	1602	1602	vim	0.3	0.3	0:00.08	20	0	152828	6248	2548	S	1
1243	1243	python	0.3	0.3		20	0				S	1										S	1		

# Vulnerabilities

- Quarterly security patches
- Deployment server/client
  - [SVD-2022-0608](#), [SVD-2022-0607](#)
- TLS
  - [SVD-2022-0606](#), [SVD-2022-0603](#), [SVD-2022-0602](#), [SVD-2022-0601](#)
- UFs
  - [SVD-2022-0605](#)
- Risky commands
  - [SVD-2022-0604](#)
- More info:
  - [https://www.splunk.com/en\\_us/product-security.html](https://www.splunk.com/en_us/product-security.html)
  - [https://lantern.splunk.com/Splunk\\_Platform/Product\\_Tips/Enterprise/Upgrading\\_Splunk\\_Enterprise](https://lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise)



A terminal window showing system statistics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, RUID, RUSER, RUID, RUSER, RUID, RUSER. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUID	RUSER	RUID	RUSER	RUID	RUSER
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3888	splunk	3888	3888	splunk	3888
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	72	tcpdump	72	72	tcpdump	72
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named	25
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1028	dan	1028	1028	dan	1028

# Deployment Server/Client

Deployment servers allow client publishing of bundles (SVD-2022-0608)

- Super bad
- Allows anything on your network to tell the DS to publish an app
- No detection searches
- Mitigate yesterday!
- Backported to 8.1 and 8.2 (the only one of these that was)

Deployment servers allow unauthenticated bundle access (SVD-2022-0607)

- Anyone can grab apps
- Previous pass4symmkey implementation not effective
- New pass4symmkey, but requires v9 clients
- Certificate validation

```
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSSD  RSSM  RSSV  RSSP  RSSC  RSSD  RSSM  RSSV  RSSP  RSSC
0.3  splunk  1000    0:02.80  4.3  20  0  135356  43956  8948  S  1  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888
0.3  tcpdump  72     0:02.45  0.7  20  0  28588  6872  5464  S  1  72  72  72  72  72  72  72  72  72  72  72  72
0.3  named    25     7:31.12  1.8  20  0  548272  18872  5584  S  1  25  25  25  25  25  25  25  25  25  25  25
0.3  dan     1028    0:00.08  0.6  20  0  152828  6248  2548  S  1  25  25  25  25  25  25  25  25  25  25  25
```

# TLS

- [SVD-2022-0606, SVD-2022-0603, SVD-2022-0602, SVD-2022-0601](#)
- All present similar issues, that is, Splunk wasn't validating certificates correctly
- New TLS docs!
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/AboutsecuringyourSplunkconfigurationwithSSL](#)

```
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python
```

%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2880	splunk	2880	2880	splunk	2880	2880	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	72	tcpdump	72	72	tcpdump
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named	25	25	named
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1028	dan	1028	1028	dan	1028	1028	dan

# Universal Forwarders

- [SVD-2022-0605](#)
- Once you set a password, remote login is allowed by default
- Splunk 9 changes that
- No longer binding to all IPs, just localhost
- You can pull the same trick on older versions

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	PID	USER	%CPU	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	%CPU	MEM	PR	NI	VIRT	RES	SHR	S
32616	32616	splunkd	0.3	4.3	20	0	135356	43956	8948	S	1	32616	splunkd	0.3	4.3	20	0	135356	43956	8948	S
32695	32695	tcpdump	0.3	0.7	20	0	28588	6872	5464	S	32695	32695	tcpdump	0.3	0.7	20	0	28588	6872	5464	S
590	590	named	0.3	1.8	20	0	548272	18872	5584	S	1	25	named	0.3	1.8	20	0	548272	18872	5584	S
1602	1602	vim	0.3	0.6	20	0	152828	6248	2548	S	38588	1602	vim	0.3	0.6	20	0	152828	6248	2548	S
1243	1243	python	0.3	0.6	20	0	152828	6248	2548	S	38588	1243	python	0.3	0.6	20	0	152828	6248	2548	S

# Risky ~~Business~~ Commands

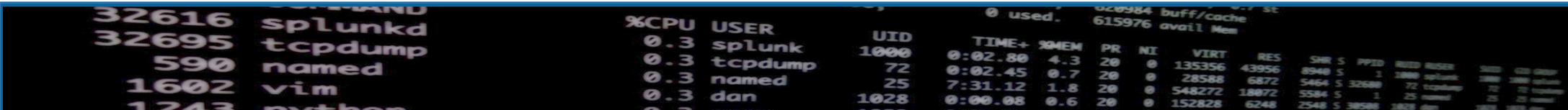
- [SVD-2022-0604](#)
- Attacker using a compromised browser could inject commands
- Turn off your GUIs (indexers, for example, maybe your DS)
- [New capabilities in Splunk 9](#)

```
COMMAND
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSIZE  RMEM  ...
0.3 splunk  1000    0:02.80 4.3  20  0  135356 43956 8940 S  1  2880  splunk  1000  1000  splunk
0.3 tcpdump  72     0:02.45 0.7  20  0  28588  6872  5464 S  1  72  tcpdump  72  72  tcpdump
0.3 named    25     7:31.12 1.8  20  0  548272 18872 5584 S  1  25  named    25  25  named
0.3 dan     1028   0:00.08 0.6  20  0  152828  6248  2548 S  1  38584  1828  dan    25  25  dan
```

# Audit improvements/Config Tracking

- New internal index, `_configtracker`, only admin can search by default
- Some fields are ignored, if they are sensitive
- Monitors:
  - `$(SPLUNK_HOME)/etc/system`
  - `$(SPLUNK_HOME)/etc/apps`
  - `$(SPLUNK_HOME)/etc/users`
  - `$(SPLUNK_HOME)/etc/slave-apps`
  - `$(SPLUNK_HOME)/etc/instance.cfg`
- You can add configs you want ignored
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/WhatSplunklogsaboutitself#Configuration Change Tracker](https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/WhatSplunklogsaboutitself#Configuration%20Change%20Tracker)



The image shows a terminal window with system metrics and a process list. The top part displays memory usage: '0 used' and '615976 avail Mem'. Below that is a table of system metrics with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The bottom part shows a list of processes with columns: PID, USER, and process name.

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

PID	USER	Process Name
32616	splunkd	splunkd
32695	tcpdump	tcpdump
590	named	named
1602	vim	vim
1243	python	python

# Universal Forwarder Security Improvements

- Config changes now monitored by default
- Windows Managed Service Accounts
- Automatic password generation on Windows
- Linux use of capabilities for a least-privilege install
  - <https://docs.splunk.com/Documentation/Forwarder/9.0.0/Forwarder/Install/eastprivileged>
- Management interface now binds to localhost by default
- Native collection of MacOS Unified Logging

```
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python
```

%CPU	USER	UID	TIME+	PMEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	STATE	TIME	MEM
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	3888	splunk	3888	3888	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	72	tcpdump	72	72	tcpdump
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1028	dan	38588	1028	dan

# Role-based fields

- Preview feature. Currently provided “as is”, no support
- Can filter or mask
- Allows you to mask fields using SEDCMD-like syntax for obfuscation
- Can replace with hashes to allow for value-based searches/stats
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/setfieldfiltering>

```
0 used, 615976 avail Mem
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RUID  RUSER  ST  TID  TNAME
32616 splunkd   0        0:02.80 4.3    20  0  135356 43956 8948 S  1  2888 splunkd 2888 2888 splunkd
32695 tcpdump   0        0:02.45 0.7    20  0  28588  6872 5464 S  1  2888 tcpdump 2888 2888 tcpdump
 590 named    0        7:31.12 1.8    20  0  548272 18872 5584 S  1  25 named 25 25 named
1602 vim      0        0:00.08 0.6    20  0  152828  6248 2548 S  38588 1828 vim 1828 1828 vim
1243 python  0        0:00.00 0.0    20  0  152828  6248 2548 S  38588 1828 python 1828 1828 python
```

# Indexing

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	USER	MEM	PR	NI	VIRT	RES
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk	1000	20	0	135356	43956
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	1	tcpdump	72	20	0	28588	6872
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named	25	20	0	548272	18872
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	1	dan	1028	20	0	152828	6248

# Indexing

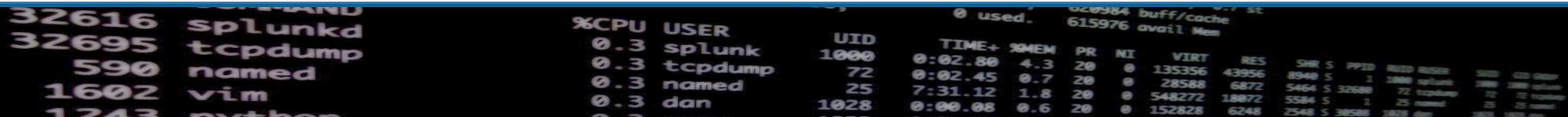
- Ingest Actions
- Indexer Manager HA
- Bucket Merging
- Azure SmartStore
- TSIDX compression in SmartStore
- TSIDX writing level

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	PPID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	
32616	splunkd	0.3		0:02.80	20	0	135356	43956	8940	S	1	3880	splunk	0.3	4.3	20	0	28588	6872	5464	S	1
32695	tcpdump	0.3		0:02.45	20	0	28588	6872	5464	S	72	tcpdump	0.3	0.7	20	0	548272	18872	5584	S	1	
590	named	0.3		7:31.12	20	0	548272	18872	5584	S	25	named	0.3	1.8	20	0	152828	6248	2548	S	38588	
1602	vim	0.3		0:00.08	20	0	152828	6248	2548	S	25	vim	0.3	0.6	20	0						
1243	python	0.3																				

# Ingest Actions

- Biggest change to the Splunk pipelines since 7.3
- Allows you more flexibility with data
- You can drop, mask, route (including S3!)
- Competes with Cribl, sort of
- Like TRANSFORMS, SEDCMD, but with a shiny interface (with previews, sometimes)
- Index Manager and Deployment Server deployment methods
- Even works on cooked events!

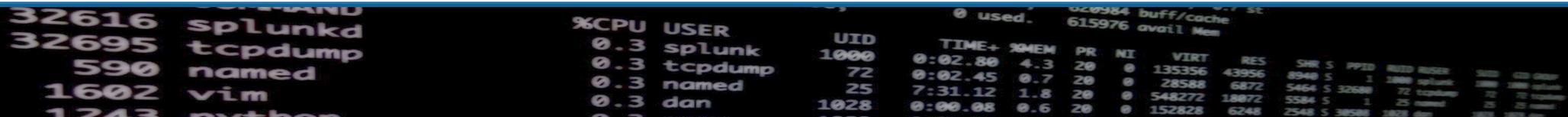


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The table lists processes like splunkd, tcpdump, named, vim, and dan.

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

# Ingest Actions - pipeline changes

- Uses the existing regexreplace processor
- Also hooked up from the TCP in for cooked events
- Applies after other transforms
- New DestinationKey in indexing pipelines for output to S3
- S3 only works on AWS, saves to a format called "HEC json"
- Can be used for re-ingest, but no index-time fields other than standard metadata (minus index)
- New metrics (disabled by default, can enable per ruleset)



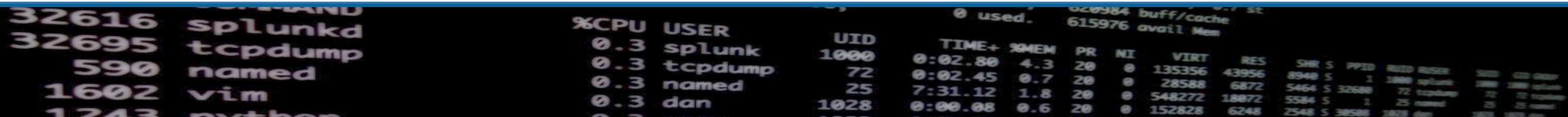
A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, NAME. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	NAME
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	tcpdump
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	python



# Ingest Actions – Deployment (CM)

- Interface on Cluster Manager allows for preview and deployment
- Interface allows S3 config
- Deployment is just the standard bundle push, so look out for undeployed changes!
- New rulesets don't require rolling restart, but change/remove does (right now)
- New app: splunk\_ingest\_actions
- New capabilities: list\_ingest\_ruleset, edit\_ingest\_ruleset

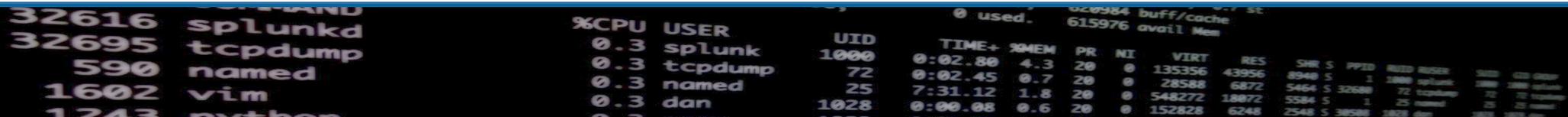


A terminal window showing system metrics and a list of processes. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, RUID, RGRP, and RPID.

PID	COMMAND	%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER	RGROUP	RUID	RGRP	RPID
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	/usr	splunk	splunk	1000	splunk	32616
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	/usr	tcpdump	tcpdump	72	tcpdump	32695
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/usr	named	named	25	named	590
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	vim	vim	1028	vim	1602
1243	python	0.3	python	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	python	python	1028	python	1243

# Ingest Actions – Deployment (DS)

- No configuration of S3
- Only supports HF (pipelines may be on UFs, but not tested)
- Currently only supports 10 HFs
- Dedicated DS
- Even visiting the UI creates a new serverclass “IngestAction\_AutoGenerated”
- Careful adding rulesets to a TA and then deploying it from your normal DS or to everywhere. Double processing is a thing.

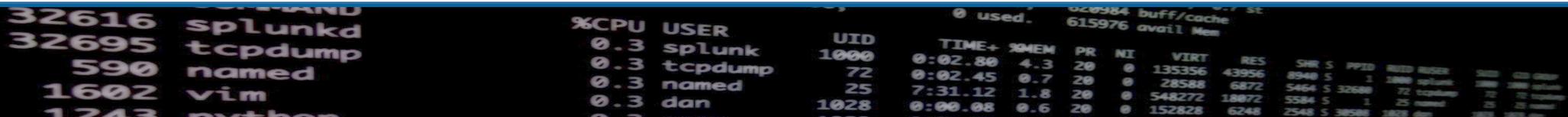


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

# Cluster Manager HA

- CM was a single point of failure
- Used to have to sync/failover manually, but some things were in memory, so left behind
- Uses an active/passive topology
- Bundles, generation, peers get synced (bucket list not included)
- Configurable heartbeat
- With a load balancer in front of your CM, this can be automated
- Can also be done with DNS entries, but that would be manual
- New tab in the Indexer Clustering dashboard shows status (in a passive node, that is all you get)
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/CMredundancy>



The image shows a terminal window with two sections of output. The top section shows system status information, including memory usage (0 used, 615976 avail Mem) and a list of processes. The bottom section shows a detailed process list with columns for PID, CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, and RES.

PID	CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248
1243	0.3	python							

# Bucket Merging

- cluster-merge-buckets command
- Can be used to merge smaller buckets for a reduced overall bucket count
- Covers DMA
- Dry run, backup, runtime limitations
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/CommandlinetoolsforusewithSupport#:~:text=cluster%2Dmerge%2Dbuckets,the%20old%20buckets%20are%20removed>

```
COMMAND
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 other

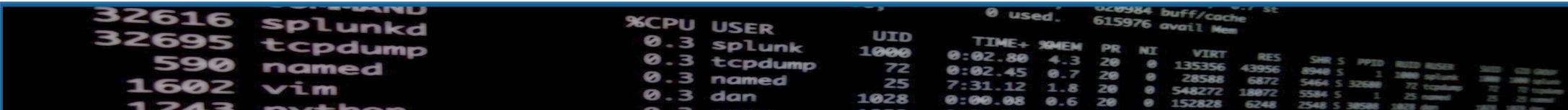
%CPU USER      UID      TIME+  MEM     PR  NI  VIRT  RES
0.3 splunk  1000    0:02.80 4.3 20  0 135356 43956
0.3 tcpdump 72      0:02.45 0.7 20  0 28588 6872
0.3 named   25      7:31.12 1.8 20  0 548272 18872
0.3 dan    1028    0:00.08 0.6 20  0 152828 6248
```





# TSIDX writing level

- Controls the format of the TSIDX files
- Enhancements have been made over the years, version dependent
- Now defaults to 3 (was 2)
- Max is 4
- Older indexers can't read the newer levels
- Check the chart in docs for version compatibility
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Reducesidxdiskusage#The\\_tsidx\\_writing\\_level](https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Reducesidxdiskusage#The_tsidx_writing_level)



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

# Admin

```
020984 buff/cache 0 used, 615976 avail Mem
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RUSR  RDSR  ST
32616 splunkd    1000     0:02.80 4.3   20  0  135356 43956 8940 S  1  2880 splunkd  2880  2880 splunkd
32695 tcpdump    72      0:02.45 0.7   20  0  28588  6872  5464 S  72  tcpdump  72  72  tcpdump
590  named      25      7:31.12 1.8   20  0  548272 18872 5584 S  1  25  named  25  25  named
1602 vim        1028    0:00.08 0.6   20  0  152828  6248  2548 S  38584 1828 vim  1828  1828 vim
1243 python
```



# Admin

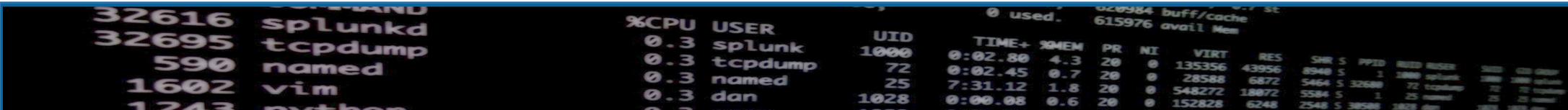
- Splunk Assist
- KVStore upgrade
- Readiness App and Python 3
- Health Report and Monitoring Console
- Workload management
- Biased Language

```
020984 buff/cache 0 used, 615976 avail Mem
```

PID	PPID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	PPID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	
32616		splunkd	0.3		0:02.80	20	0	135356	43956	8948	S	1	splunkd	0.3		0:02.45	20	0	28588	6872	5464	S	1
32695		tcpdump	0.3		7:31.12	20	0	548272	18872	5584	S	1	named	0.3		0:00.08	20	0	152828	6248	2548	S	1
590		named	0.3																				
1602		vim	0.3																				
1243		python	0.3																				

# Splunk Assist

- Cloud based service, can be used from on-prem
- Uses telemetry data, so you have to be sending that (Usage Data)
- Net new offering
- In the Monitoring Console
- Needs to be activated
- Tied to your enterprise license
- Can't be used on FIPS instances or in docker
- Current features:
  - TLS cert checking is a feature that jumps out:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/UseCertAssist>
  - Config assist:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/UseConfigAssist>



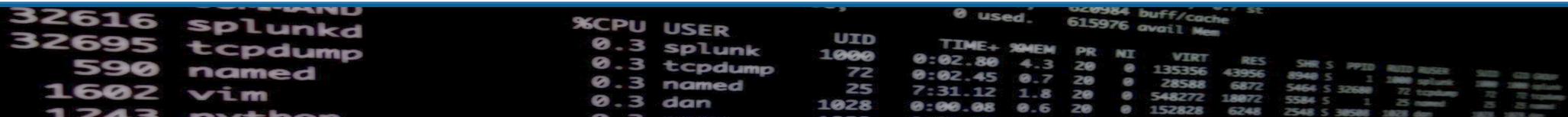
A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248



# Readiness App and Python 3

- Splunk Upgrade Readiness App now at version 4
- Prepares for Python 3 and jQuery framework changes
- Can scan for issues
- There is no Python 2 in Splunk 9
- Checks TLS configurations (inbound and outbound in Python)
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/UpgradeReadiness/About>

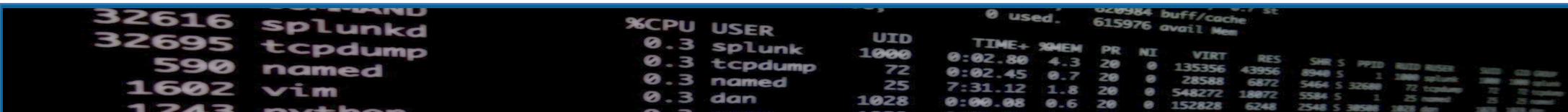


A terminal window showing system statistics and a list of processes. The top part shows memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, RUID, RGRP, RUID, RGRP.

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER	RGROUP	RUID	RGRP	RUID	RGRP
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	/usr	splunk	splunk	splunk	splunk	splunk	
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	/72	tcpdump	tcpdump	tcpdump	tcpdump	tcpdump	
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/	named	named	named	named	named	
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	vim	vim	vim	vim	vim	
1243	python	0.3	python	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	python	python	python	python	python	

# Health Report and Monitoring Console

- Better descriptions of indicators and what they mean
- New forwarder latency indicator
- Also looks for potential config issues
- Alerts can now be snoozed
- Alerts can be emailed to admins
  - [https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configurealerts#Set up health report alert actions](https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configurealerts#Set_up_health_report_alert_actions)
- Monitoring Console now can automatically build your asset list
  - [https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configureindistributedmode#Enable automatic distributed mode configuration](https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configureindistributedmode#Enable_automatic_distributed_mode_configuration)



A terminal window showing system status and process information. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, RSESSION, RUID, RUSERGROUP, RUSERSESSION.

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER	RGROUP	RSESSION	RUID	RUSERGROUP	RUSERSESSION
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	/usr	splunk	splunk	splunk	1000	splunk	splunk
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	/usr	tcpdump	tcpdump	tcpdump	72	tcpdump	tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/usr	named	named	named	25	named	named
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	vim	vim	vim	1028	vim	vim
1243	python	0.3	python	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr	python	python	python	1028	python	python

# Workload management

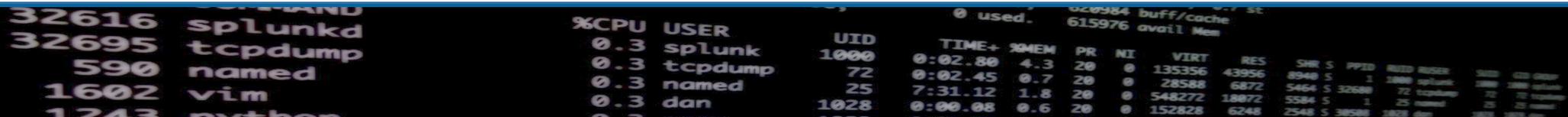
- More options for more flexibility
- Roles and indexes now support wildcards
- Can set limits on Ad doc searches
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Workloads/WorkloadRules>

```
0 used, 615976 avail Mem
```

PPID	PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	STATE	TIME	MEM
32616	32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	1000	splunkd	0	0:02.80	4.3
32695	32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	1	72	tcpdump	0	0:02.45	0.7
590	590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	0	7:31.12	1.8
1602	1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	1	1028	vim	0	0:00.08	0.6
1243	1243	0.3	python															

# Biased Language

- This has been a long running project at Splunk
- Started a few releases ago
- IDXC, Licensing, allow and deny lists
- There is backwards compatibility, but older config directives may be removed, there are a lot of notes in the docs around this
- Note that you can't use both
- Path changes: master-apps -> manager-apps, slave-apps -> peer-apps
  - [https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Updatepeerconfigurations#Which\\_directory\\_to\\_use:\\_manager-apps\\_or\\_master-apps.3F](https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Updatepeerconfigurations#Which_directory_to_use:_manager-apps_or_master-apps.3F)
- The old terms still remain in logs as there are customers that use them in multiple ways. Logging may change once more of the effort is complete
- In MC, there are server roles that may need to be updated



The image shows a terminal window with system status information and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes.

PID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunkd
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30588	vim
1243	python	0.3												

# Search

```
020984 buff/cache 0 used, 615976 avail Mem
```

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUSER	RUID	GROUP
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk	splunk	splunk
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named	named	named
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30584	1028	dan	dan

# Search

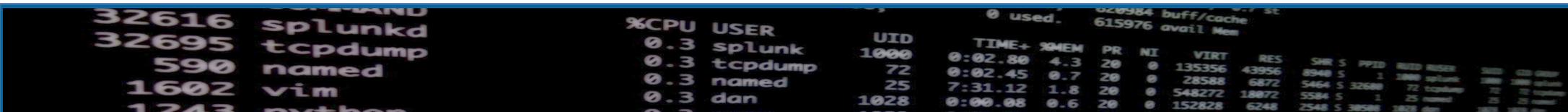
- Federated Search
- Geoip DB

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	MEM	MEM	MEM
32616	32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3880	splunk	3880	3880	splunk
32695	32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	72	tcpdump
590	590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named
1602	1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	1602	vim	1602	1602	vim
1243	1243	0.3	python															

# Federated Search

- Federated Search != Hybrid Search:  
<http://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Hybrid2Federated>
  - Hybrid = peering to other CM/indexers
  - Federated Search = connecting via remote SH
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Aboutfederatedsearch>
- Better UI with options for restrictions for knowledge objects to limit bundle replication
- Now options for Splunk Cloud -> On prem FS
- Can now use tstats, data models, DMA, lookups
- Transparent Federated Search
  - No more writing in special commands or syntax
  - Only runs in fast mode, so no search-time fields
  - No real-time searching
  - Has to be Transparent or Standard mode, not mixed



A terminal window showing system statistics and a list of processes. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, TTY, T, TTYNAME, and ST.

PID	COMMAND	%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER	RGROUP	TTY	T	TTYNAME	ST
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	/usr	splunk	splunk		00		
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	/	tcpdump	tcpdump		00		
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/	named	named		00		
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/	vim	vim		00		
1243	python	0.3	python	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/	python	python		00		

# Geoip DB

- No longer using MaxMind as the provider
- The format is the same
- Now using an open source provider
- If you are using a subscription from MaxMind, it will still work

```
0 used, 615976 avail Mem
```

	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RSSD	RSSK	...
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2880	...	...
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	...	...
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	...	...
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38580	1828	...	...
1243	0.3	python	...	...	...	...	...	...	...	...	...	...	...	...	...

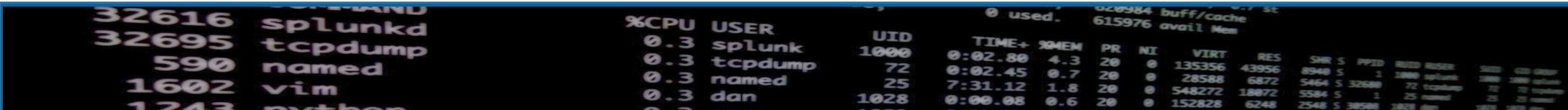
# Other stuff

```
020984 buff/cache 0 used, 615976 avail Mem
```

COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUSER	RUID	GROUP
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk	splunk	splunk
32695 tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	tcpdump
590 named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named	named	named
1602 vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30584	1028	dan	dan
1243 pytho															

# Other stuff

- Dashboards
  - Syntax changes for visualizations
  - No more inline stylesheets
  - Lots of changes to Dashboard Studio:  
<https://docs.splunk.com/Documentation/Splunk/9.0.0/DashStudio/WhatNew>
- jQuery
  - Admins can disable jQuery 2 access
- Splunk Secure Gateway App
  - New version, lots of changes to make mobile access better
- Semantic versioning of APIs
  - Makes writing things using Splunk APIs easier and more stable, allows for targeting a specific version, and gentle deprecation of older versions
  - <https://semver.org/>



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, and others. The processes listed include splunkd, tcpdump, named, vim, and others.

PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	OTHER
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	3888
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	72
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1602
1243	0.3	others											